

Базовые понятия ИБ

Определения обновлены по **актуальным** нормативным источникам. В колонке "Определение (актуальное)" — действующая формулировка. В колонке "Определение (ГОСТ 17090, историческое)" — первоначальная формулировка из ГОСТ Р ИСО 17090-1-2015 для сравнения.

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
Авторизация (<i>authorization</i>)	Санкционирование доступа — предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ. [ГОСТ Р 58833-2020, п. 3.2; Р 50.1.056-2005; ГОСТ Р 57580.1-2017]	Процесс предоставления субъекту полномочий, в том числе предоставление доступа на основе полномочий доступа. [ИСО 7498-2:1989 Заменён]
Актив (<i>asset</i>)	Всё, что имеет ценность для организации. К активам относятся: информация, ПО, материальные активы (компьютеры), услуги, люди и их квалификация, нематериальные активы (репутация, имидж). [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.2; ГОСТ Р 53114-2008; СТО БР ИББС-1.0-2014]	—
Аудит безопасности (<i>security audit</i>)	Проверка реализованных в системе процедур обеспечения безопасности с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию. [Р 50.1.053-2005; ГОСТ 33707-2016]	—
Аудит информационной безопасности (<i>information security audit</i>)	Систематический, независимый и документированный процесс получения свидетельств аудита и их объективной оценки для определения степени, в которой выполняются критерии аудита ИБ. [ГОСТ Р 53114-2008, п. 3.5.3]	—
Аутентификация (<i>authentication</i>)	Обеспечение гарантии того, что заявленные характеристики субъекта и объекта являются подлинными. [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.5] Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора и	Процесс надёжной идентификации субъекта информационной безопасности путём защищённой ассоциации, установленной между идентификатором и субъектом. [ГОСТ Р ИСО

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
	аутентификационной информации. [ГОСТ Р 58833-2020, п. 3.4]	17090-1-2015, ИСО 7498-2:1989 Заменён
Безопасность информации (<i>information security</i>)	Состояние защищённости информации, при котором обеспечиваются её конфиденциальность, целостность и доступность. [ГОСТ Р 50922-2006, п. 2.4.5]	Состояние защищённости, при котором обеспечиваются доступность, конфиденциальность, целостность и учётность. [ENV 13608-1 Заменён на EN 13608-1]
Безопасность информационной технологии (<i>ICT security</i>)	Состояние защищённости информационной технологии, при котором обеспечивается выполнение изделием, реализующим информационную технологию, предписанных функций без нарушений безопасности обрабатываемой информации. [P 50.1.056-2005, п. 3.1.4]	—
Безопасность автоматизированной информационной системы (<i>automated system security</i>)	Состояние защищённости автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов. [P 50.1.053-2005, п. 3.1.6]	—
Взаимная аутентификация (<i>mutual authentication</i>)	Обоюдная аутентификация, обеспечивающая для каждого из участников процесса аутентификации уверенность в том, что другой участник является тем, за кого себя выдаёт. [ГОСТ Р 58833-2020, п. 3.10]	—
Вторичная идентификация (<i>secondary identification</i>)	Действия по проверке существования (наличия) идентификатора, предъявленного субъектом доступа при доступе, в перечне идентификаторов доступа, которые были присвоены субъектам доступа и объектам доступа при первичной идентификации. [ГОСТ Р 58833-2020, п. 3.12]	—
Доверенная третья сторона (<i>trusted third party</i>)	Участник процесса аутентификации, предоставляющий один или более сервисов в области защиты информации, которому доверяют другие участники процесса аутентификации как поставщику данных услуг. [ГОСТ Р 58833-2020, п. 3.15]	—
Доверенный объект (<i>trusted object</i>)	Объект, который будет действовать в полном соответствии с ожиданиями и субъекта доступа, и объекта доступа или любого из них, при этом	—

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
	выполняя то, что он должен делать, и не выполняя то, что он не должен делать. [ГОСТ Р 58833-2020, п. 3.14]	
Доверие (assurance)	Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности. [ГОСТ Р 58833-2020, п. 3.16, ГОСТ Р 54581-2011]	—
Доступ (access)	Получение одной стороной информационного взаимодействия возможности использования ресурсов другой стороны информационного взаимодействия. [ГОСТ Р 58833-2020, п. 3.17]	—
Доступность (availability)	Свойство, определяющее возможность использования объекта авторизованным субъектом по запросу. [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.7] Состояние информации, при котором обеспечивается возможность её получения и использования за разумное время. [ГОСТ Р 50922-2006, п. 2.5.3]	Свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта. [ИСО 7498-2:1989 Заменён]
Закрытый ключ (private key)	Ключ из состава асимметричной пары ключей, сформированных для объекта, который должен быть использован только этим объектом. [ГОСТ Р 58833-2020, п. 3.18]	—
Закрытый ключ неизвлекаемый (non-extractable private key)	Закрытый ключ, который при его формировании и хранении невозможно извлечь из устройства аутентификации, в котором он был создан. [ГОСТ Р 58833-2020, п. 3.19]	—
Защищаемая автоматизированная информационная система (protected automated system)	Автоматизированная информационная система, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем её защищённости. [П 50.1.053-2005, п. 3.1.1]	—
Защищаемые информационные ресурсы (protected information resources)	Информационные ресурсы автоматизированной информационной системы, для которых должен быть обеспечен требуемый уровень их защищённости. [П 50.1.053-2005, п. 3.1.2]	—

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
Значимый объект критической информационной инфраструктуры (ЗОКИИ)	Объект критической информационной инфраструктуры, которому в установленном порядке присвоена одна из категорий значимости. Включение в реестр значимых объектов влечёт обязанность категорирования, передачу сведений во ФСТЭК России и выполнение дополнительных требований защиты. Федеральный закон от 26.07.2017 № 187-ФЗ, ст. 2, п. 7; приказ ФСТЭК России от 21.12.2017 № 235 —	
Идентификатор (<i>identifier</i>)	Признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесённую с ними идентификационную информацию. [ГОСТ Р 58833-2020, п. 3.20]	Информационный объект, используемый для объявления идентичности перед тем, как получить подтверждение соответствия от определённого аутентификатора. [ENV 13608-1 Заменён]
Идентификация (<i>identification</i>)	Действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов. [ГОСТ Р 58833-2020, п. 3.24] Выполнение проверок, позволяющих системе обработки данных распознавать объекты. [ИСО/МЭК 2382-8:1998 Заменён] — исторический вариант.	Выполнение проверок, позволяющих системе обработки данных распознавать объекты. [ИСО/МЭК 2382-8:1998 Заменён]
Информативный сигнал (<i>informative signal</i>)	Сигнал, по параметрам которого может быть определена защищаемая информация. [Р 50.1.053-2005, п. 3.2.6]	—
Информационная безопасность объекта информатизации	Состояние защищённости объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств её обработки. [Р 50.1.056-2005, п. 3.1.1]	—
Информационная безопасность организации (<i>information security of organization</i>)	Состояние защищённости интересов организации в условиях угроз в информационной сфере. [ГОСТ Р 53114-2008, п. 3.2.1]	—
Информационная сфера	Совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор,	—

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
	формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. [ГОСТ Р 53114-2008, п. 3.1.3]	
Информационная инфраструктура	Совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам. [ГОСТ Р 53114-2008, п. 3.1.4]	—
Инцидент безопасности (<i>information security incident</i>)	Одно или серия нежелательных или неожиданных событий безопасности информационной, имеющих значительную вероятность нарушения бизнес-операций или представляющих угрозу для безопасности информационной. [ГОСТ Р ИСО/МЭК ТО 18044:2007; СТО БР ИББС-1.0-2014; ГОСТ Р 53114-2008]	—
Источник угрозы безопасности информации	Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации. [Р 50.1.056-2005, п. 3.2.2]	—
Компьютерная атака (<i>attack</i>)	Целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств. [Р 50.1.056-2005, п. 3.2.8]	—
Контроль доступа (<i>access control</i>)	Обеспечение санкционированного доступа к активам в соответствии с бизнес-требованиями и требованиями безопасности. [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.1] Управление доступом — средства, с помощью которых ресурсы предоставляются только авторизованным субъектам. [ГОСТ Р 58833-2020, п. 3.18]	Средства, с помощью которых ресурсы системы обработки данных предоставляются только авторизованным субъектам в соответствии с установленными правилами. [ИСО/МЭК 2382-8:1998 Заменён]
Контроль обеспечения ИБ (<i>information security control</i>)	Проверка соответствия состояния информационной безопасности организации установленным требованиям. [ГОСТ Р 53114-2008, п. 3.5.1]	—
Конфиденциальность (<i>confidentiality</i>)	Недоступность информации для неавторизованных лиц, объектов или процессов. [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.10]	Свойство информации быть недоступной и закрытой для неавторизованного лица,

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
	Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё права. [ГОСТ Р 50922-2006, п. 2.5.1]	логического объекта или процесса. [ИСО 7498-2:1989 Заменён]
Конфиденциальность, целостность, доступность (КЦД)	Три базовых свойства защищаемой информации, обеспечиваемые совместно средствами защиты информации (классическая триада ИБ, англ. CIA triad). Защита информации по определению есть состояние защищённости, при котором обеспечиваются именно эти три свойства. [ГОСТ Р 50922-2006, п. 2.4.5]	—
Критически важная система информационной инфраструктуры	Объект информационной инфраструктуры, нарушение функционирования которого может привести к серьёзным последствиям. [ГОСТ Р 53114-2008, п. 3.1.15]	—
Менеджмент информационной безопасности (<i>information security management</i>)	Скоординированные действия по руководству и управлению организацией в области информационной безопасности. [ГОСТ Р 53114-2008, п. 3.4.1]	—
Менеджмент риска информационной безопасности (<i>information security risk management</i>)	Скоординированные действия по руководству и управлению организацией в отношении риска ИБ с целью его снижения. Основные процессы: установление контекста, оценка риска, обработка и принятие риска, мониторинг. [ГОСТ Р 53114-2008, п. 3.4.2]	—
Мера безопасности (<i>security measure</i>)	Мера защитная — средство или действие, направленное на предотвращение или снижение риска реализации угроз информационных. Включает организационные и технические меры. [ГОСТ Р 57580.1-2017; СТО БР ИББС-1.0-2014]	—
Многофакторная аутентификация (<i>multi-factor authentication</i>)	Аутентификация, при выполнении которой используется не менее двух различных факторов аутентификации. [ГОСТ Р 58833-2020, п. 3.29]	—
Модель угроз (<i>threat model</i>)	Физическое, математическое, графическое или иное описание угроз безопасности информации, а также объектов и процессов, в отношении которых они могут быть реализованы. [ГОСТ Р 53114-2008, п. 3.3.3]	—

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
Нарушение информационной безопасности	Случайное или преднамеренное неправомерное действие физического лица в отношении активов организации, следствием которого является нарушение безопасности информации при её обработке техническими средствами, вызывающее негативные последствия (ущерб/вред) для организации. [ГОСТ Р 53114-2008, п. 3.2.4]	—
Национальный координационный центр по компьютерным инцидентам (НКЦКИ)	Центр, осуществляющий координацию деятельности субъектов критической информационной инфраструктуры по выявлению, предупреждению и ликвидации последствий компьютерных атак и компьютерных инцидентов, а также взаимодействие с зарубежными и международными организациями в этой сфере; функции НКЦКИ осуществляет ФСБ России. Федеральный закон от 26.07.2017 № 187-ФЗ, ст. 20.2; Указ Президента РФ от 15.02.2024 № 121 —	
Неоспоримость (<i>non-repudiation</i>)	Нет самостоятельного определения в действующих ГОСТ серии 27000. Термин используется в контексте криптографической защиты. [ГОСТ Р ИСО 17090-1-2015]	Услуга, обеспечивающая каждой из участвующих сторон доказательство целостности и происхождения данных (неразрывно друг от друга). [ГОСТ Р ИСО 17090-1-2015]
Несанкционированное воздействие (НСВ)	Изменение, уничтожение или копирование информации [ресурсов информационной системы], осуществляемое с нарушением установленных прав и (или) правил. [Р 50.1.056-2005, п. 3.2.7]	—
Несанкционированный доступ (НСД) (<i>unauthorized access</i>)	Доступ к информации [ресурсам информационной системы], осуществляемый с нарушением установленных прав и (или) правил доступа к информации [ресурсам информационной системы] с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному назначению и техническим характеристикам. [Р 50.1.056-2005, п. 3.2.6]	—
Объект доступа (<i>access object</i>)	Одна из сторон информационного взаимодействия, предоставляющая доступ. [ГОСТ Р 58833-2020, п. 3.33]	—
Объект защиты информации	Информация или носитель информации, или информационный процесс, который необходимо защищать в соответствии с целью защиты	—

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
	информации. [ГОСТ Р 53114-2008, п. 3.2.2, ГОСТ Р 50922-2006]	
Объект информатизации	Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений и объектов, в которых они установлены. [ГОСТ Р 53114-2008, п. 3.1.5]	—
Организационные меры обеспечения ИБ (organizational security measures)	Меры обеспечения ИБ, реализуемые через организационные решения — политики, процедуры, инструкции, регламенты. [ГОСТ Р 53114-2008, п. 3.6.4]	—
Отказ в обслуживании (denial of service)	Несанкционированное блокирование доступа к информации [ресурсам информационной системы] — создание условий, препятствующих доступу к информации [ресурсам информационной системы] субъекту, имеющему право на него. [Р 50.1.056-2005, п. 3.2.10]	—
Открытый ключ (public key)	Ключ из состава асимметричной пары ключей, сформированных для объекта, который может быть общедоступным. [ГОСТ Р 58833-2020, п. 3.39]	—
Оценка соответствия ИБ (information security compliance assessment)	Определение соответствия состояния ИБ организации установленным требованиям и оценка эффективности реализованных мер. [ГОСТ Р 53114-2008, п. 3.5.5]	—
Первичная идентификация (primary identification)	Действия по формированию и регистрации информации о субъекте доступа или объекте доступа, а также действия по присвоению идентификатора доступа субъекту доступа или объекту доступа и его регистрации в перечне присвоенных идентификаторов доступа. [ГОСТ Р 58833-2020, п. 3.41]	—
Перехват информации (interception)	Неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов. [Р 50.1.053-2005, п. 3.2.5]	—
Подлинность (authenticity)	Состояние ресурсов информационной системы, при котором обеспечивается реализация информационной технологии с использованием	—

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
	именно тех ресурсов, к которым субъект, имеющий на это право, обращается. [P 50.1.056-2005, п. 3.1.10]	
Показатель защищённости информации	Количественная или качественная характеристика безопасности информации, определяющая уровень требований, предъявляемых к конфиденциальности, целостности и доступности этой информации и реализуемых при её обработке. [P 50.1.056-2005, п. 3.1.11]	—
Политика безопасности (<i>information security policy</i>)	Политика в области информационной безопасности — официально утверждённые руководством правила и процедуры, обеспечивающие достижение целей ИБ. [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.44]	Утверждённый план или способ действий по обеспечению информационной безопасности. [ИСО/МЭК 2382-8:1998 Заменён]
Правила разграничения доступа (<i>access control rules</i>)	Совокупность правил, регламентирующих права доступа субъектов к объектам доступа в автоматизированной информационной системе. [P 50.1.053-2005, п. 3.2.8]	—
Простая аутентификация (<i>simple authentication</i>)	Аутентификация с применением метода однофакторной односторонней аутентификации и соответствующих данному методу протоколов аутентификации. [ГОСТ Р 58833-2020, п. 3.46]	—
Риск безопасности ИБ (<i>information security risk</i>)	Сочетание вероятности реализации угрозы и её последствий для активов организации. [ГОСТ Р 51897-2011; ГОСТ Р 53114-2008]	—
Санкционированный доступ (<i>authorized access</i>)	Доступ субъекта доступа к объекту доступа, не нарушающий правила управления доступом. [ГОСТ Р 58833-2020, п. 3.51]	—
Система менеджмента информационной безопасности (СМИБ) (<i>information security management system</i>)	Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения ИБ. [ГОСТ Р 53114-2008, п. 3.4.3, ГОСТ Р ИСО/МЭК 27000-2021]	—

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
Служба безопасности (<i>security service</i>)	Нет самостоятельного определения в действующих ГОСТ серии 27000. Понятие заменено на "меры безопасности" (security controls). [ГОСТ Р ИСО/МЭК 27000-2021 — не включён]	Служба, предоставляемая уровнем взаимодействия открытых систем и обеспечивающая адекватную защиту систем или передачи данных. [ИСО 7498-2:1989 Заменён]
Среда функционирования (<i>operating environment</i>)	Среда с предопределёнными (установленными) граничными условиями, в которой существуют (функционируют) и взаимодействуют субъекты доступа и объекты доступа. [ГОСТ Р 58833-2020, n. 3.53]	—
Средство обнаружения вторжений (<i>intrusion detection system</i>)	Программное или программно-техническое средство, автоматизирующее процесс обнаружения атак на ресурсы информационной системы. [ГОСТ Р 53114-2008, n. 3.6.6]	—
Средство защиты от НСД (<i>unauthorized access protection</i>)	Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации. [ГОСТ Р 53114-2008, n. 3.6.7]	—
Строгая аутентификация (<i>strong authentication</i>)	Аутентификация с применением только метода многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации. [ГОСТ Р 58833-2020, n. 3.54]	—
Субъект доступа (<i>access subject</i>)	Одна из сторон информационного взаимодействия, которая инициирует получение и получает доступ. [ГОСТ Р 58833-2020, n. 3.55]	—
Техническая защита информации (ТЗИ) (<i>technical protection</i>)	Деятельность, направленная на обеспечение некриптографическими методами безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств. [Р 50.1.056-2005, n. 3.1.2]	—
Техническое средство обеспечения ИБ (<i>technical security measure</i>)	Оборудование, приборы, устройства, аппаратно-программные комплексы, обеспечивающие защиту информации техническими и программно-	—

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
	техническими средствами. [ГОСТ Р 53114-2008, п. 3.6.5]	
Уверенность (<i>confidence</i>)	Убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (корректно, надёжно, эффективно, в соответствии с политикой безопасности). [ГОСТ Р 58833-2020, п. 3.56, ГОСТ Р 54581-2011]	—
Угроза безопасности информации (<i>information security threat</i>)	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. [ГОСТ Р 50922-2006; ГОСТ Р 56545-2015; ПНСТ-799-2022] Совокупность условий и факторов, создающих опасность нарушения конфиденциальности, доступности и (или) целостности информации. [Р 50.1.053-2005; Р 50.1.056-2005]	—
Управление доступом (<i>access management</i>)	Предоставление санкционированного и предотвращение несанкционированного доступа. [ГОСТ Р 58833-2020, п. 3.57]	—
Уровень доверия (<i>assurance level</i>)	Степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия. [ГОСТ Р 58833-2020, п. 3.58, ГОСТ Р 54581-2011]	—
Усиленная аутентификация (<i>enhanced authentication</i>)	Аутентификация с применением метода многофакторной односторонней или взаимной аутентификации и соответствующих данному методу протоколов аутентификации. [ГОСТ Р 58833-2020, п. 3.59]	—
Утечка информации по техническому каналу (<i>information leakage</i>)	Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. [Р 50.1.053-2005, п. 3.2.4]	—
Учётность (<i>accountability</i>)	Нет самостоятельного определения в действующих ГОСТ серии 27000. Связанные термины: "ведение записей" (log records), "регистрация событий безопасности" (audit logging). [ГОСТ Р 59548-2022 "Регистрация событий безопасности"]	Свойство, обеспечивающее однозначное отслеживание действий логического объекта. [ИСО 7498-2:1989 Заменён]

Термин / Англ.	Определение (актуальное)	Определение (ГОСТ 17090, историческое)
Уязвимость (<i>vulnerability</i>)	Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами. [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.61; ГОСТ Р 50922-2006; ГОСТ Р 53113.1-2008] Недостаток или слабое место в системе автоматизированной информационной, которые могут быть условием реализации угрозы безопасности обрабатываемой в ней информации. [Р 50.1.053-2005]	—
Фактор (<i>factor</i>)	Вид (форма) существования информации, используемой при идентификации и аутентификации. [ГОСТ Р 58833-2020, п. 3.61]	—
Целостность (<i>integrity</i>)	Свойство информации сохранять точность и полноту, а также способность системы защиты информации обеспечивать неизменность информации. [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.34] Состояние информации, при котором отсутствует любое её изменение или изменениями обеспечивается их неискажённость (введены изменения только теми субъектами и в то время, когда это разрешено). [ГОСТ Р 50922-2006, п. 2.5.2]	Доказательство, что содержание сообщения не было каким-либо способом случайно или преднамеренно изменено при передаче сообщения. [ИСО 7498-2:1989 <i>Заменён</i>]
Целостность данных (<i>data integrity</i>)	Свойство данных не подвергаться несанкционированному изменению или уничтожению. [ГОСТ Р ИСО/МЭК 27000-2021, п. 3.34 — как аспект целостности]	Свойство данных не подвергаться несанкционированному изменению или уничтожению. [ИСО 7498-2:1989 <i>Заменён</i>]
Целостность ресурсов информационной системы	Состояние ресурсов информационной системы, при котором их изменение осуществляется только преднамеренно субъектами, имеющими на него право, при этом сохраняются их состав, содержание и организация взаимодействия. [Р 50.1.056-2005, п. 3.1.7]	—
Электронное удостоверение (<i>electronic credential</i>)	Совокупность идентификационной информации и аутентификационной информации (или прямого указания её существования) субъекта доступа или объекта доступа, подлинность которой подтверждена доверенной третьей стороной. [ГОСТ Р 58833-2020, п. 3.62]	—

